III. REMARKS

1. Applicant appreciates the Examiner's indication of allowable subject matter in claim 11. However, for the reasons stated herein, Applicant believes all of the claims to be allowable in their present form.

2. Claim 24 is amended to address the 35 U.S.C. §112, second paragraph rejection.

3. Claims 1, 3-5, 8-10, 13, 19, 20, 22 and 28-30 are not unpatentable over Federrath in view of Sayers et al. ("Sayers") and Menezes under 35 U.S.C. §103(a).

Claim 1 is directed to authenticating a mobile node to a packet data network and recites "providing the packet data network with **authentication information usable by the telecommunications network**, the authentication information comprising a challenge and a session secret corresponding to the mobile node identity and derivable using the challenge and the shared secret". This is not disclosed or suggested by the combination of Federrath, Sayers and Menezes.

Federrath discloses a GSM system and especially focuses on the alleged security threats in the GSM. Federrath discloses that the GSM system comprises one-sided authentication.

Federrath discloses the use of challenge - response (RAND - SRES) mechanism, for authentication, using a SIM card. The problem Federrath seeks to solve does not relate to the over-the-air

communications in GSM between the terminal and base station, but rather to eaves-dropping the links within the radio access network (in the core network) and to attacking the SIM by a person possessing the PIN code.

The Examiner acknowledges that Federrath does not disclose or suggest each feature of Applicant's invention. Specifically, the Examiner notes that Federrath lacks:

1) authenticating to a packet data network (p. 4, l. 13-14)

2) providing the mobile node with a protection code, and

3) cryptographically forming authentication information based on the protection code obtained from the mobile node and based on authentication information usable by a telecommunications network.

Sayers does not overcome at least these deficiencies of Federrath.

Sayers discloses a private GSM/IP network, basically implementing a private GSM network all in IP. (See e.g. Cols. 17-19 and Fig. 9.) Sayers simply establishes a private GSM network so that a normal GSM terminal can be used, (col. 10, lines 31-40), capable of operating both in private and public networks. Sayers discloses a particular system in which a mobile station may be used to connect either to commercial cellular or private networks. (See Col. 10, lines 31 to 14). Sayers makes use of the same telecommunication system, that is, GSM as Federrath, and also makes use of the same of encryption mechanism. All that Sayers may add is that GSM can be used as a radio access mechanism and to access further private networks. This is not what is claimed by Applicant. Sayers can be seen to merely

disclose one GSM network interoperating with the others only so that this network employs IP in data exchange between its network elements. The air interface is that of GSM.

However, Applicant's invention relates to authenticating a terminal to a packet data network. The Sayers network is not seen by the terminal as a packet data network if the terminal communicates with it only using circuit switched data known from GSM. Applicant's invention, as recited in the claims, differs from Sayers at least in not actually authenticating to a packet data network, but to a telecommunications network. In Sayers' system, a normal GSM phone would believe it connects to an ordinary GSM network when it connects to Sayers' private network. Subsequently, no shared secret known to the telecommunications network is used to authenticate to a packet data network as is claimed by Applicant. In Sayers, the authentication must match that of GSM and thus lacks the use of the terminal based protection code. Thus, Federrath and Sayers do not disclose or suggest each feature of Applicant's invention as claimed.

Additionally, Sayers does not disclose or suggest an actual telecommunications network, but only represents one possible alternative for telecommunications. Even if it were possible to formulate a link which a person ordinarily skilled in the art could have come to think of combining Sayers and Federrath, for instance, it is respectfully asserted that the motivation to do so is speculative, and is rather based on hindsight reasoning with knowledge of Applicant's invention.

Menezes, in combination with Federrath and Sayers, does not overcome the above-noted deficiencies. Menezes describes that random numbers can be used in challenge-response protocols. This

is also known from GSM authentication where RAND is a nonce. Menezes shows a general level description of challenge-response authentication but does not relate to improving an existing authentication system.

Applicant's invention provides a robust authentication method without necessitating changes to the SIM or HLR of the existing telecommunications networks.

Menezes might be used when creating a totally new authentication system, requiring also new types of SIMs and HLR's, i.e. new algorithms. This could be useful on designing entirely new telecommunications systems such as when UMTS where USIM and UMTS-HLR were designed.

Applicant's invention on the other hand, allows using the existing authentication mechanism as a base and improves the system using the existing primitives and interfaces of SIM cards and HLRs.

Thus, the combination of Federrath, Sayers and Menezes does not disclose or suggest each feature of Applicant's invention.

The Examiner's suggestion as to the motivation to combine references is respectfully traversed.

Both Sayers and Federrath already make use of the fundamentals of cryptographic discussed by the Handbook of Applied Cryptography written by Menezes. There is no motivation or suggestion to use this handbook to provide a new extra security mechanism on top of GSM. Instead, if a person skilled in the art would have wanted to combine these references she might have ended up designing an

entirely new communications system that makes use of mutual authentication.

Menezes would not motivate a person ordinarily skilled in the art to modify GSM to achieve Applicant's invention, because the basics of cryptography are understood by the developers of GSM. Even if advantages could be gained from a more sophisticated authentication, the prior existence of even superior methods does not in itself suffice to prove that a person skilled in the art would, not could, have desired to combine the teachings of Federrath, Sayers and Menezes so as to arrive at Applicant's invention as recited in the claims. Thus, it is submitted that a *prima facie* case of obviousness over Federrath, Sayers and Menezes cannot be and is not established. Therefore, claims 1, 3-5, 8-10, 13, 19, 20, 22 and 28-30 are patentable over the combination of Federrath, Sayers and Menezes.

4. Claim 2 is not unpatentable over Federrath in view of Sayers and Menezes and further in view of Aboba, under 35 U.S.C. §103(a), at least in view of its dependency on claim 1.

5. Claims 6-7 are not unpatentable over Federrath in view of Sayers and Menezes and further in view of Brown, under 35 U.S.C. §103(a), at least in view of their respective dependencies.

Furthermore, Brown discloses only the use of a SIM card for authentication in different telecom systems and using a challenge and response. Thus, Brown does not disclose or suggest each feature of Applicant's invention as claimed.

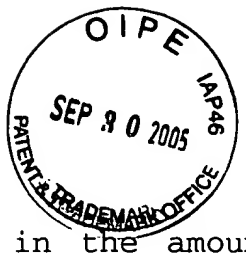
6. Claim 12 is not unpatentable over Federrath in view of Sayers and Menezes and further in view of Harkins under 35 U.S.C. §103(a), at least in view of its dependency.

7. Claims 15, 17, 18 and 26 are not unpatentable over Federrath in view of Sayers, Menezes and Abrol under 35 U.S.C. §103(a). The arguments recited above with respect to claim 1 are equally applicable with respect to claims 15, 17, 18 and 26. Furthermore, Abrol only shows that a gateway can deliver authentication protocol information to mobile users employing e.g. CHAP or MIP. Abrol does not disclose or suggest that improvements for an existing authentication system would be used as described in Applicant's invention.

Thus, the claims should be allowable.

8. Claim 25 is not unpatentable over Federrath, Sayers, Menezes, Abrol and Harkins and Schneir under 35 U.S.C. §103(a) at least by reason of its dependency.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.



A check in the amount of $450.00 is enclosed for a two-month extension of time. The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,

Geza C. Ziegler, Jr.
Reg. No. 44,004

28 September 2005
Date

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800 Ext. 134
Customer No.: 2512

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date indicated below as first class mail in an envelope addressed to MAIL STOP AMENDMENT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: Sept. 28, 2005

Signature: Meaghan Baye
Person Making Deposit